Listing of Claims

1. (Currently amended) A method of determining random values for an a stream cipher, comprising:

determining at least two sequential random values ~~for the stream cipher~~ in parallel utilizing a common S-box.

2. (Original) The method of Claim 1, wherein the step of determining at least two sequential random values in parallel utilizing a common S-box further comprises the steps of:

determining if a collision exists between accesses of the common S-box utilized to determine a first of the two sequential random values and accesses of the common S-box utilized to determine a second of the two sequential random values; and

modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box.

3. (Currently amended) The method of Claim 2, wherein the step of determining if a collision exists comprises the steps of:

determining a state associated with the determination of the at least two sequential random values;

comparing values of counters utilized in determining the at least two sequential random values; and

detecting a collision based on the determined state and the compared values.

4. (Original) The method of Claim 3, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the step of detecting a collision comprises the steps of:

detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

detecting a second collision if the determined state is the first state and the second j

counter values equals the first i counter value;

detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

detecting a fourth collision if the determined state is the second state, the second j counter values equals the first t counter value; and

detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

5. (Original) The method of Claim 4, wherein the step of modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box comprises the steps of:

utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

6. (Original) The method of Claim 2, further comprising the steps of:

determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the